How the Russia-Ukraine conflict affects the local cyber threat landscape

By Nithen Naidoo

14 Mar 2022

Hybrid warfare, using cyber as a vector, has not only blurred boundaries between nations but also between war and peace; friend and foe; and the virtual world and reality.

Source: Maksim Shmeljov - 123RF.com

As tensions increase following Russia's invasion of Ukraine, the threat of state-sponsored cyber-attacks is a growing concern.

Proficiency in signal intelligence, espionage and mass cognitive influence, built over decades of covert and overt conflict, has translated into a formidable cyber warfare capability for many countries like Russia, the United States, China, Israel, North Korea and Iran.

Africa's ability to defend against such a rapidly evolving asymmetric force requires a foundation of high-fidelity intelligence.

A recent industry survey found that most businesses consider themselves unaffected by the Ukraine crisis in terms of changes in their cyber threat landscape.

There has been an increase in opportunistic attacks from other nation-states and cybercriminal groups trying to exploit the crisis using the "fog of war" to conduct and obfuscate attacks.

The recent attack on the Mozambique government's infrastructure is one such example. Additionally, there has been a notable increase in targeted phishing attacks, business email compromise (BEC), online scams and disinformation campaigns.

This raises the questions: what are the root causes of these contradictory views? And what insights can we glean from this analysis to improve intelligence processing?

There are three core contributing factors that influence the varying views regarding the dynamics of the threat landscape:

Siloed view

Many businesses have a siloed view of their threat landscape which translates into an inability to leverage or share intelligence with external cyber threat intelligence entities such as a central industry authority or national computer security incident response teams.

Such businesses fail to identify the correlation between an indiscriminate attack and a potential threat targeting their industry or critical national information infrastructure.

Growing list of retail brands suspend business in Russia [updated]

Lauren Hartzenberg 11 Mar 2022

This highlights the need for greater industry, cross-vertical and national intelligence sharing.

Low and slow

The second is the "low and slow" nature of state-sponsored activities.

The sheer volume of events and alerts generated, from the vast amount of data consumed and communicated in business today is cognitive overload for a human analyst.

This is why many security staff struggle with analyst and decision fatigue. Nation-state adversaries understand and leverage this complexity by ensuring they remain within the bounds of an acceptable threshold of attack.

Active defence, cyber AI and automation augment the work done by analysts by automatically responding to clearly explicit, high-volume cyber threats.

This reduces the noise and administrative overhead while simultaneously amplifying signals and intelligence.

Attribution

This leads us to the third factor – the challenge of attribution. The clear benefits of cyber as a vector in hybrid warfare are economies of force, ease of scale, and anonymity.

Nation-state attacks are rarely initiated from a nation's own IP space and often leverage novel attack vectors and custom tooling which go to great lengths to conceal their identity and avoid detection.

Additionally, many state-sponsored threat actors deploy "false flag" strategies, not only as a smokescreen but to further their political agenda and help achieve strategic objectives.

Apple could lose R46m in iPhone sales daily amid Russia market exit

7 Mar 2022

Threat and vulnerability intelligence needs to be viewed through a wider lens, beyond traditional indicators of compromise and attack data feeds.

Although static blacklisting defences have their place, there is a clear need to analyse and understand threats more intimately.

This includes threats unique to the African landscape, which do not feature in international data feeds, such as those emanating from the likes of organised crime syndicates like Black Axe and internet fraudsters Yahoo Boys.

This not only enhances static defences but also empowers your tactical and strategic edge.

ABOUT THE AUTHOR

Nithen Naidoo is CEO and co-founder of Snode Technologies.